Lecture 23: Quadratic Forms III
Reduction Theory

William Stein

Math 124 Harvard University **Fall 2001**

Recall that a binary quadratic form is a function $f(x, y) = ax^2 + bxy + cy^2$. Our motivating problem is to decide which numbers are "represented" by f; i.e., for which integers n do there exist integers x, y such that $ax^2 + bxy + cy^2 = n$? If $g \in \mathrm{SL}_2(\mathbb{Z})$ then $f(x, y)$ and $f|_g(x, y) = f\left(g \begin{bmatrix} x \\ y \end{bmatrix}\right)$ represent exactly the same set of integers. Also, $\mathrm{disc}(f) = \mathrm{disc}(f|_g)$, where $\mathrm{disc}(f) = b^2 - 4ac$, and f is called *positive definite* if $\mathrm{disc}(f) < 0$ and $a > 0$.

In today's lecture, we will learn about reduction theory, which allows us to decide whether or not two positive definite binary quadratic forms are equivalent under the action of $\mathrm{SL}_2(\mathbb{Z})$.

If, in the future, you would like to pursue the theory of binary quadratic forms in either a more algebraic or algorithmic direction, I highly recommend that you look at Chapter 5 of Henri Cohen's book *A Course in Computational Algebraic Number Theory* (GTM 138).

1 Reduced Forms

Definition 1.1 (Reduced). A positive definite quadratic form (a, b, c) is *reduced* if $|b| \leq a \leq c$ and if, in addition, when one of the two inequalities is an equality (i.e., either $|b| = a$ or $a = c$), then $b \geq 0$.

There is a geometric interpretation of reduced, which we will not use this later. Let $D = \mathrm{disc}(a, b, c) = b^2 - 4ac$ and set $\tau = \frac{-b+\sqrt{D}}{2a}$, so τ is the root of $ax^2 + bx + c$ with positive imaginary part. The right action of $\mathrm{SL}_2(\mathbb{Z})$ on positive definite binary quadratic forms corresponds to the left action of $\mathrm{SL}_2(\mathbb{Z})$ by linear fractional transformations on the complex upper half plane $\mathfrak{h} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. The standard fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{h}$ is

$$\mathcal{F} = \left\{\tau \in \mathfrak{h} : \mathrm{Re}(\tau) \in \left[-\frac{1}{2}, \frac{1}{2}\right), |\tau| > 1 \text{ or } |\tau| = 1 \text{ and } \mathrm{Re}(\tau) \leq 0\right\}.$$

Then (a, b, c) is reduced if and only if the corresponding complex number τ lies in $\mathcal{F}$. For example, if (a, b, c) is reduced then $\mathrm{Re}(\tau) = -b/2a \in [-1/2, 1/2)$ since $|b| \leq a$

and if $|b| = a$ then $b \geq 0$. Also

$$|\tau| = \sqrt{\frac{b^2 + 4ac - b^2}{4a^2}} = \sqrt{\frac{c}{a}} \geq 1$$

and if $|\tau| = 1$ then $b \geq 0$ so $\mathrm{Re}(\tau) \leq 0$.

The following theorem (which is not proved in Davenport) highlights the importance of reduced forms.

Theorem 1.2. *There is exactly one reduced form in each equivalence class of positive definite binary quadratic forms.*

Proof. We have to prove two things. First, that every class contains at least one reduced form, and second that this reduced form is the only one in the class.

We first prove that there is a reduced form in every class. Let $\mathcal{C}$ be an equivalence class of positive definite quadratic forms of discriminant D. Let (a, b, c) be an element of $\mathcal{C}$ such that a is minimal (amongst elements of $\mathcal{C}$). Note that for any such form we have $c \geq a$, since (a, b, c) is equivalent to $(c, -b, a)$ (use the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$). Applying the element $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ to (a, b, c) for a suitably chosen integer k (precisely, $k = \lfloor (a - b)/2a \rfloor$) results in a form (a', b', c') with $a' = a$ and $b' \in (-a', a']$. Since $a' = a$ is minimal, we have just as above that $a' \leq c'$, hence (a', b', c') is "just about" reduced. The only possible remaining problem would occur if $a' = c'$ and $b' < 0$. In that case, changing (a', b', c') to $(c'', b'', a'') = (c', -b', a')$ results in an equivalent form with $b'' > 0$, so that (c'', b'', a'') is reduced.

Next suppose (a, b, c) is a reduced form. We will now establish that (a, b, c) is the only reduced form in its equivalence class. First, we check that a is minimal amongst all forms equivalent to (a, b, c). Indeed, every other a' has the form $a' = ap^2 + bpr + cr^2$ with p, r coprime integers (see this by hitting (a, b, c) by $\left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$). The identities

$$ap^2 + bpr + cr^2 = ap^2 \left(1 + \frac{b}{a}\frac{r}{p}\right) + cr^2 = ap^2 + cr^2 \left(1 + \frac{b}{c}\frac{p}{r}\right)$$

then imply our claim since $|b| \leq a \leq c$ (use the first identity if $r/p < 1$ and the second otherwise). Thus any other reduced form (a', b', c') equivalent to (a, b, c) has $a' = a$. But the same identity implies that the only forms equivalent to (a, b, c) with $a' = a$ are obtained by applying a transformation of the form $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ (corresponding to $p = 1$, $r = 0$). Thus $b' = b + 2ak$ for some k. Since $a = a'$ we have $b, b' \in (-a, a]$, so $k = 0$. Finally

$$c' = \frac{(b')^2 - D}{4a'} = \frac{b^2 - D}{4a} = c,$$

so $(a', b', c') = (a, b, c)$. $\square$

2 Finding an Equivalent Reduced Form

Here is how to find the reduced form equivalent to a given positive definite form (a, b, c). This algorithm is useful for solving problems 8 and 9 on the homework assignment. Consider the following two operations, which can be used to diminish one of a and $|b|$, without altering the other:

1. If $c < a$, replace (a, b, c) by the equivalent form $(c, -b, a)$.
2. If $|b| > a$, replace (a, b, c) by the equivalent form (a, b', c') where $b' = b + 2ka$ and k is chosen so that $b' \in (-a, a]$ (more precisely, $k = \lfloor \frac{a-b}{2a} \rfloor$), and c' is found from the fact that $(b')^2 - 4ac' = D = \mathrm{disc}(a, b, c)$, so $c' = \frac{(b')^2 - D}{4a}$.

Starting with (a, b, c), if you iterate the appropriate operation, eventually you will find the reduced form that is equivalent to (a, b, c).

Example 2.1. Let $f = 458x^2 + 214xy + 25y^2$.

Equivalent form	What I did	Matrix
$(458, 214, 25)$		
$(25, -214, 458)$	(1)	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$(25, -14, 2)$	(2) with $k = 4$	$\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right)$
$(2, 14, 25)$	(1)	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$(2, 2, 1)$	(2) with $k = -3$	$\left(\begin{smallmatrix} 1 & -3 \\ 0 & 1 \end{smallmatrix}\right)$
$(1, -2, 2)$	(1)	$\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$
$(1, 0, 1)$	(2) with $k = 1$	$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

Let

$$\begin{aligned} g &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 4 \\ -13 & -17 \end{pmatrix}. \end{aligned}$$

Then

$$f|_g = x^2 + y^2!$$

3 Some PARI Code

The following PARI code checks whether or not a form is reduced, and computes the reduced form equivalent to a given form. You can download it from my web page if you don't want to type it in.

```
\\ true if and only if (a,b,c) is reduced.
{isreduced(a,b,c) =
   if(b^2-4*a*c>=0 || a<0,
      error("reduce: (a,b,c) must be positive definite."));
   if(!(abs(b)<=a && a<=c), return(0));
   if(abs(b)==a || a==c, return(b>=0));
   return(1);
}
```

```
\\ reduces, printing out each step.  returns the reduced form
\\ and a matrix that transforms the input form to the reduced form.
{reduce(a,b,c,s) =
   local(D, k, t, g);
   D=b^2-4*a*c;
   if(D>=0 || a<0, error("reduce: (a,b,c) must be positive definite."));
   g=[1,0;0,1];
   while(!isreduced(a,b,c),       \\ ! means ``not''
      if(c<a,
         b = -b; t = a; a = c; c = t;
         g = g*[0,-1;1,0];
         print([a,b,c], "  \t(1)"),  \\ backslash t means ``tab''
      \\ else
         if (abs(b)>a || -b==a,
            k = floor((a-b)/(2*a));
            b = b+2*k*a;
            c = (b^2-D)/(4*a);
            g = g*[1,k;0,1];
            print([a,b,c], "  \t(2) with k=",k)
         )
      )
   );
   return([a,b,c,g])
}

/* Here is an example:
? \r quadform
? reduce(458,214,25)
[25, -214, 458] (1)
[25, -14, 2]    (2) with k=4
[2, 14, 25]     (1)
[2, 2, 1]       (2) with k=-3
[1, -2, 2]      (1)
[1, 0, 1]       (2) with k=1
%22 = [1, 0, 1, [3, 4; -13, -17]]
*/
```